REMARKS

In view of the ensuing discussion, the Applicants submit that none of the claims now pending in the application is obvious under the provisions of 35 USC § 103.

If, however, the Examiner believes that there are any unresolved issues requiring adverse final action in any of the claims now pending in the application, the Examiner should telephone Mr. Peter L. Michaelson, Esq. at (732) 542-7800 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Status of claims

No claims have been amended, canceled or added.

Rejections under 35 USC § 103

A. Claims 21-25 and 28-31

The Examiner has rejected claims 21-25 and 28-31 under the provisions of 35 USC § 103 as being obvious over the teachings in the '866 Bruwer et al patent (United States patent 5,841,866 issued to F. J. Bruwer et al on November 24, 1998). This rejection is respectfully traversed. To simplify the discussion, this rejection will be primarily discussed in the context of independent claim 21 from which all the remaining claims depend.

Specifically, the Examiner takes the position that, with one exception, all the limititations recited in claim 21 are disclosed in the '866 Bruwer et al patent. As to that exception, the Examiner states that the '866 Bruwer et al patent discloses that communication occurs between a terminal and a card rather than from the card, through the terminal, to a server. The Examiner recognizes that, pursuant to MPEP § 2144.04, merely separating something, here being the terminal, into components, i.e., a terminal portion and a server, would be obvious. Consequently, with the teachings of the Bruwer et al patent and that recognition in mind, the Examiner concludes that the invention, as recited in claim 21, would be obvious to a person of ordinary skill in the art at the time of the present invention for the reason that such a person would utilize the server to maintain a central database through which the validity of requests could be checked. The Examiner implicitly concludes that such a hypothetical combination would yield the Applicants' invention recited in claim 21. As the Examiner will soon appreciate, this view is incorrect.

Significant, fundamental differences, which the Examiner did not recognize, exist betwen the methodology taught by the '866 Bruwer et al patent and that of the present invention as recited in claim 21.

To appropriately elucidate these differences in a manner that facilitates their ready understanding, the Applicants will first summarize the salient teachings of the present invention, then summarize the salient teachings in the

'866 Bruwer et al patent, and finally contrast those teachings of the two in a manner which delineates the basic differences therebetween.

As described in the Applicants' prior amendment (mailed May 27, 2009), the present invention is directed to activating a card, here being a chipcard, used to obtain services through a communications network from a service provider.

Activation is accomplished electronically through interaction among the card -- specifically circuitry (a "chip") located on the card itself, a terminal into which a user inserts the card for activation, and a remote server, connected to the terminal through appropriate communication infrastructure, for a service provider associated with the card.

Specifically, a user first obtains card 1 (as shown in FIG. 1 and discussed in page 4, line 16 et seq). However, to utilize the card to gain services from its associated service provider, the user first needs to activate the card to gain access to a predefined balance, whether monetary or otherwise, which has been given to the card and stored in the server for the service provider and in an account associated with the card. To do so, the user inserts the card into terminal 6 which communicates through infrastructure 7, containing a communications network, with remote server 8 which, in turn, accesses database 10. As indicated in FIG. 2 and described in page 5, line 4 et seq, the card contains internal storage medium 15 (on-board non-volatile memory) which stores card data,

that data containing card ID 2, activation code 3 and initial challenge code 4. The card also stores challenge 5 and result 11. Activation code 3, which differs for each card, is similar to a code that could be printed on a conventional chipcard and made visible by "scratching" an overlying surface of that card but here is stored in a secure manner within the card's memory.

As described in page 5, line 23 et seq, initial challenge 4 is a code which the server, via the communications infrastructure, provides to the card for storage within memory 15. This code is stored prior to the card being distributed to its user. During subsequent activation and as discussed below, the card returns its activation code after having received an activation challenge that is equal to its pre-stored initial challenge 4.

Challenge 5 is a code that is first a pre-defined value which has been pre-stored in the card for use during activation and subsequently a value that reflects the then current status of the card (i.e., not activated, active or empty).

In essence and as described in page 6, line 17 et seq, to activate and/or use the card, the user will insert the card into the terminal. In response, the terminal will then access the card data from memory 15 and transmit both card ID 2 and challenge 5 to the terminal.

The terminal compares challenge 5 with a predetermined code (referred to as C1, such as the value 111...1) to assess whether the card has not yet been activated. If the challenge equals C1, the terminal, sends the card ID to the server, and requests the server to send activation challenge code 9 associated with that specific card ID back to the terminal. To do so, the server appropriately accesses database 10 for a record associated with that card ID. The activation challenge code has a value, which, if identical to the initial challenge 4 stored on the card, enables the card to access the activation code that is already stored on the card. The server sends the activation challenge code to the terminal which, in turn, sends it onward to the card. The card overwrites its stored challenge 5 with the activation challenge code it received from the server.

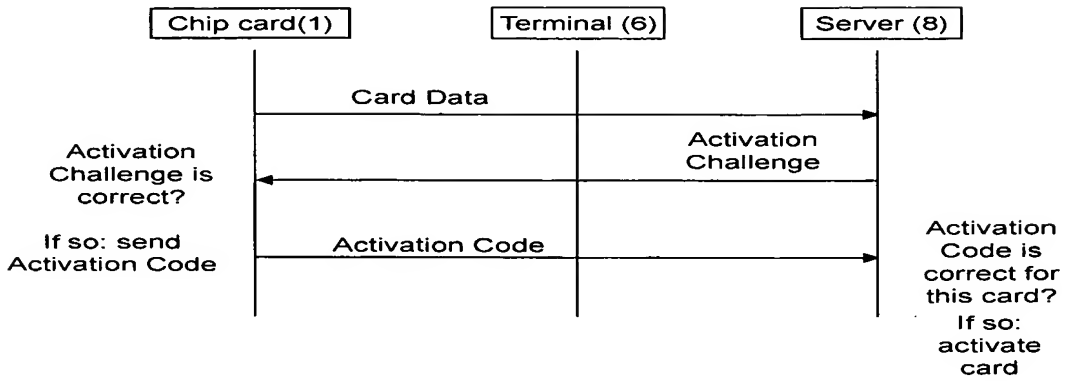
The card then compares the present value of the stored challenge (which here is now that value of the activation challenge code 9 just supplied by the server instead of code C1) with initial challenge code 4. If the two match, then the card retrieves activation code 3 from its memory and assigns the activation code to result 11. Otherwise, if the two fail to match, the card assigns a predefined error code, referred to as E1, to result 11.

In either case, the card transmits result 11 to the terminal which, in turn, sends the card ID and that result onward to the server. In response, the server checks whether the value of that result equals a value of activation code 3 which has been stored in database 10 and associated with that

card ID. If a match occurs, then the server activates a balance associated with the card, thus allowing the user of the card to obtain services through the card and from the service provider associated with the server. In doing so, the server, as a threshold matter, checks whether the result does not equal error code E1. Activation only occurs if the result does not equal this error code. As indicated in page 8, line 14 et seq, whenever the balance for the card is exhausted, the server assigns a predefined value, referred to as C2, to challenge 5. Should the card be active but its balance not exhausted, then challenge 5 has a value that is equal to neither C1 or C2 but rather to activation challenge code 9. Thus, the value of challenge 5, as stored on the card, reflects the current status of the card: not activated, active or empty. If result 11 equals error code E1, then a fraudulent activation attempt has occurred which is reflected in a difference then existing between the values of initial challenge 4 and challenge 5 as they are then both stored on the card.

Thus, the basic steps in the Applicants' inventive activation methodology are: inserting the chipcard card into a terminal, and reading card data and transmitting that data from the chipcard, via the terminal, to the server; sending an activation challenge code from the server, via the terminal to the card; determining, in the card, whether the activation challenge code is correct by comparing that code with an initial challenge code stored in the card itself; and if the activation challenge code is correct (i.e., these two match), then sending an activation code stored in the card back to the server in

order to activate a balance associated with that card. These steps are shown in graphical form as follows:



With the above in mind, a more detailed depiction of the process of activating the Applicants' chipcard is provided in FIG. 3 of the present application, which for convenience, is reproduced below.

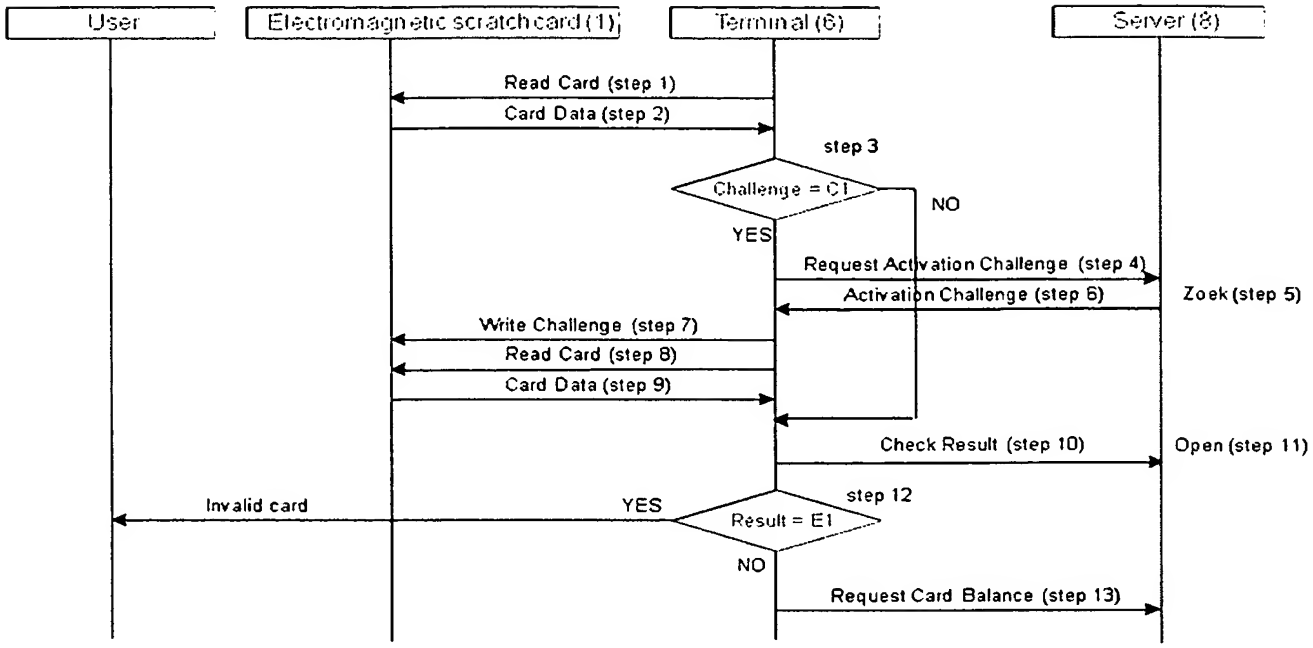


FIG. 3

The steps in the above flowchart that are particularly relevant to Claim 21 are steps 7, 8 and 9. In step 7, the terminal sends the activation challenge code to the card (the terminal has previously received this code from the server through step 6.) The card compares the activation challenge code it received with the initial challenge code stored in the card. If the card determines that these two values match, the card then, via steps 8 and 9, provides its activation code to the terminal, which, in turn, forwards it to the server which, through database access based on the card ID, determines the validity of that activation code. Presenting the correct activation challenge to the card effectively "scratches open" the card though electronically.

Thus, of crucial importance and in accordance with the Applicants' inventive teachings, the card returns its activation code if and only if it has received the correct activation challenge code from the server.

Now, apart from the severability of the terminal and server, does the Bruwer et al patent disclose the Applicants' inventive card activation process? No. As the Examiner will soon appreciate, significant and fundamental differences exist between the two.

The '866 Bruwer et al patent describes a method of authenticating a chipcard that also relies on use of a challenge-response procedure. See, e.g., col. 4, line 28 et seq of that patent. In general, and as noted in col. 5, line 5 et seq, the methodology involves the card accepting a challenge, then generating a first response (being, e.g., an encoded or hashed value -- as indicated in col. 3, line 30 et seq) to the challenge using a first algorithm which operates on the challenge and a secret key, the key being derived from information stored on the card itself. That information, as indicated in, e.g., col. 3, line 32 et seq and col. 4, line 46 et seq, may be the contents of a counter situated on the card. The terminal then validates the response, and, if valid, accepts an associated transaction then made through the card.

Consider FIG. 2 of that patent, which is as follows:

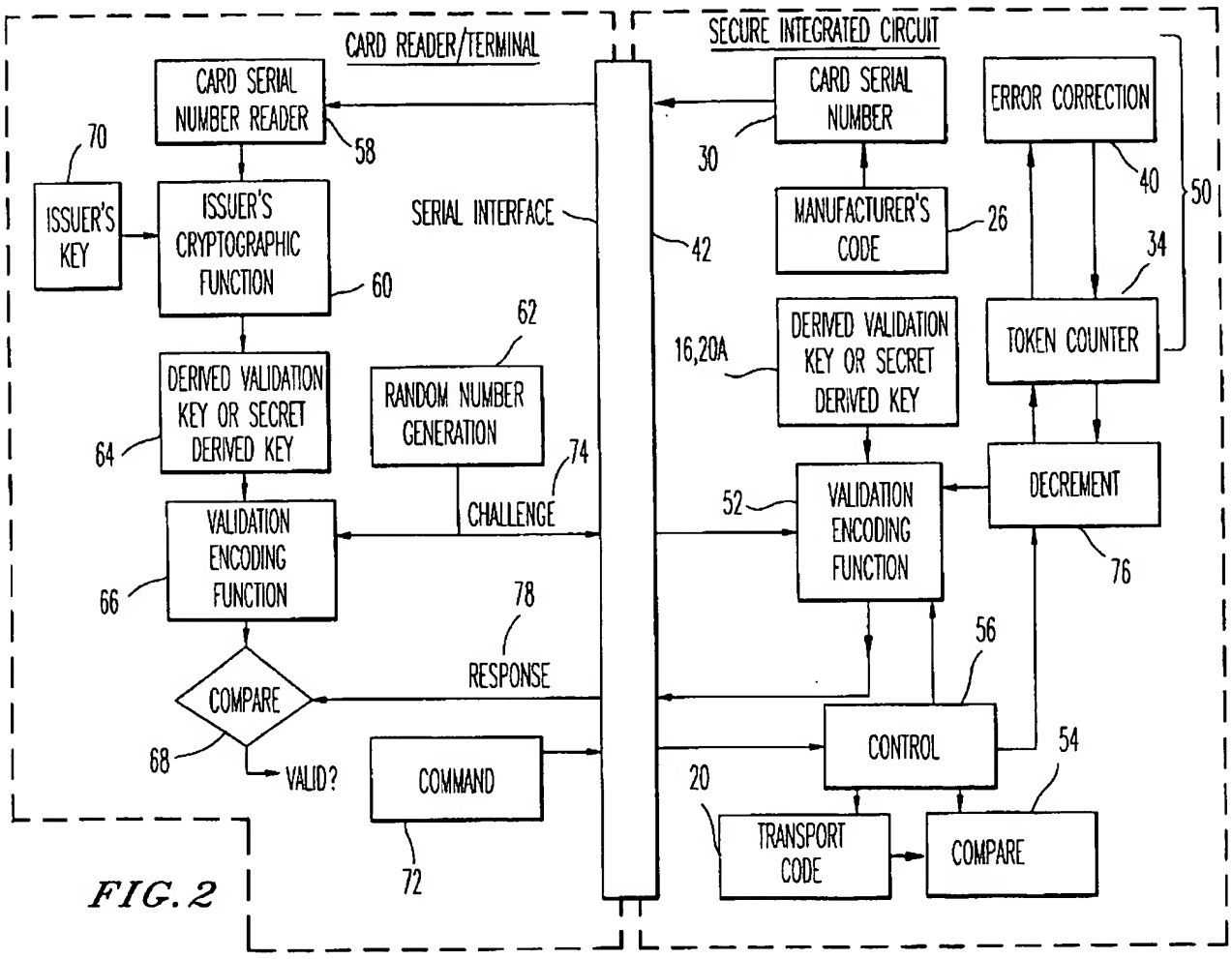


FIG. 2

The elements shown in this figure which are particularly relevant to claim 21 are:

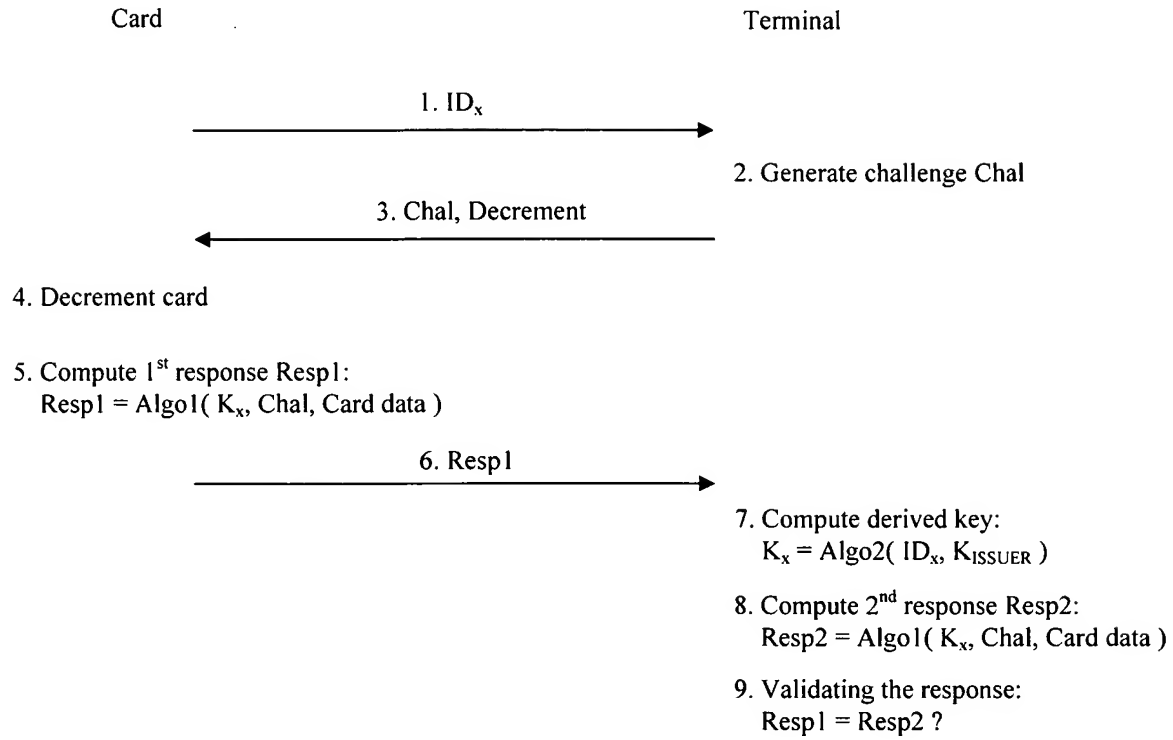
1) random number generator 62 which, in the terminal, generates random number 74 (see col. 8, lines 42-43 of the '866 Bruwer et al patent);

2) challenge 74 which is the generated random number sent as a challenge by the terminal to the card; and

3) validation encoding function 52 which computes a response to challenge 74, a secret so-called derived key and possibly other card data, e.g., contents of a counter on the card.

The card *does not check challenge 74* it receives. Rather, the card computes response 78 from challenge 74, the secret key and possibly other values, *regardless* of the value of the received challenge.

To further illustrate the differences between the methodology taught by the '866 Bruwer et al patent and that of the Applicants, the following chart depicts the steps of the former methodology, as expressly described in on col. 3, lines 20-26 and 30-37 of that patent -- passages specifically cited by the Examiner. Here and for ease of comparison with FIG. 3 of the present application, the chip card is shown on the left side of the chart; the terminal on the right side.



As illustrated and with specific references to the supporting text in the '866 Bruwer et al patent, the steps of the Bruwer methodology are as follows:

1) The terminal reads out the card ID (col. 3, line 17 and col. 5, line 65).

2) The terminal generates challenge Chal which is a random number.

3) The terminal sends the challenge Chal to the card along with a decrement command (col. 3, lines 19-20).

4) The card implements the decrement command (col. 3, line 21).

5) The card computes a first response Resp1 (col. 3, lines 30-32 and col. 6, lines 1-4) based on the challenge, a secret key, K_x, and data on the card.

6) The terminal reads the response Resp1 from the card (col. 3, lines 22-24).

7) The terminal computes the derived secret key of the card (col. 3, lines 32-34).
8) The terminal computes a second response Resp2 (col. 6, lines 6-9).
9) The terminal checks that the card has supplied a valid response by comparing Resp1 with Resp2 (col. 3, line 25 and col. 6, lines 11-12).

Here too, it is quite evident that the card *does not check the challenge (74) it receives.* Rather, the card, computes its response from the challenge and other values, *regardless* of the value of the challenge. This occurs regardless of whether the terminal were to be parsed -- as the Examiner suggests -- into separate terminal and server portions.

This operation stands in sharp contrast to the Applicants' presently inventive methodology where the card checks the challenge it receives, and does so based on the value of a challenge which has been previously stored in the card.

Thus, the '866 Bruwer et al patent fails to teach, disclose or even suggest the Applicants' presently inventive concept, as expressly recited in claim 21, of storing an initial challenge code within the card; then receiving an activation challenge code, via an communications infrastructure, from a server; and comparing, within the card, the activation challenge code with the initial challenge code to determine a match therebetween; and if a match exists, sending an activation code from the card to the server so that the server can activate a balance with the card.

Independent claim 21, as it currently stands, contains suitable recitations directed at these distinguishing features of the present invention. Specifically, this claim recites as follows, with its principal distinguishing recitations shown in a bolded typeface:

> "A method of activating a chipcard for providing services among a terminal, accessible to a service customer, an infrastructure, comprising a network, and a server connected to the infrastructure and associated with a service provider, **the chipcard having a storage medium containing an activation code and an initial challenge code,** wherein the method comprises the steps of:
>
> inserting the chipcard in the terminal, the terminal being connected, via the infrastructure, to the server;
>
> **comparing, within the chipcard, an activation challenge code, received from the server and through the infrastructure and the terminal, with the initial challenge code stored in the storage medium; and**
>
> **if the activation challenge code equals the initial challenge code, sending the activation code stored in the medium, via the terminal and the infrastructure, to the server for activating a card balance associated with the chipcard.**" [emphasis added]

Thus, the Applicants submit that this claim is <u>not</u> rendered obvious under the provisions of 35 USC § 103 by the teachings in the '866 Bruwer et al patent, whether taken singly, or in hypothetical combination, as the Examiner proposes, with

its terminal being split into separate terminal and server portions (pursuant to the separability doctrine set forth in MPEP § 2144.04).

Each of dependent claims 22-25 and 28-31 directly or indirectly depends from new independent claim 21 and recites further distinguishing aspects of the present invention over those recited in the latter claim. Hence, the Applicants submit that each of these dependent claims is also not rendered obvious by the teachings applied by the Examiner for the exact same reasons set forth above with respect to claim 21. Consequently, each of these dependent claims is also patentable under the provisions of 35 USC § 103.

Therefore, this rejection should now be withdrawn.

B. Claims 26 and 27

The Examiner has rejected dependent claims 26 and 27 under the provisions of 35 USC § 103 as being obvious over the teachings in the '866 Bruwer et al patent taken in view of those in the '078 Lebouill patent (United States patent 7,360,078 issued to G. Lebouill on April 15, 2008). Claim 27 depends from claim 26 which, in turn, depends from all of claims 21-23. Consequently, this rejection will be discussed in the context of independent claim 21. In that context, this rejection is also respectfully traversed.

The Examiner takes the position that the '866 Bruwer et al patent teaches all the limitations in claims 21-23 but, as

to claim 26, with the exception of sending an error code if authentication failed and, as to claim 27, with the exception of sending an error code and taking further action to correct the problem as indicated by the error code. For the missing teachings, the Examiner turns to the '078 Lebouill patent. The Examiner apparently concludes that by hypothetically integrating those teachings of the '078 Lebouill patent with those of the '866 Bruwer et al patent itself combined with the concept of separating the terminal taught by the latter patent into both terminal and server portions -- that combination having been applied to claims 21-23, the resulting overall combination would yield the invention as then recited in dependent claims 26 and 27. This conclusion is incorrect with respect to independent claim 21 and hence claims 26 and 27 as well.

The Examiner correctly recognizes the teachings specifically provided by the '078 Lebouill patent. However, even if these teachings were to be hypothetically combined with those others in the manner which the Examiner proposes, the teachings provided by that patent -- being solely directed to error depiction and error handling -- simply do not change the basic authentication methodology taught by the '866 Bruwer et al patent at all. The same fundamental differences, as discussed above, between that methodology and the methodology taught and claimed by the present Applicants would persist to the same extent in the resulting combination, including the teachings of the '078 Lebouill patent, as it would without those teachings.

Consequently, the Applicants submit that claim 21 is not rendered obvious over the teachings of specific art applied

in this rejection, whether those teachings are taken singly or in any combination including that posed by the Examiner.

Each of dependent claims 26 and 27 indirectly depends from independent claim 21 and recites further distinguishing features of the present invention over those recited in that independent claim. Consequently, the Applicants submit that each of these dependent claims is also not rendered obvious under the provisions of 35 USC § 103 over all these applied teachings for the same reasons set forth above with respect to claim 21.

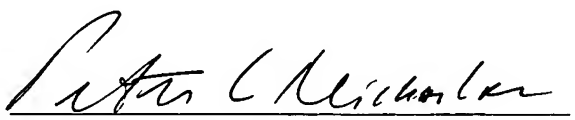
Therefore, this rejection should also be withdrawn.

Conclusion

Consequently, the Applicants believe that all their claims remain in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

Respectfully submitted,

March 1, 2010



Peter L. Michaelson, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 542-7800